Managing Double Jeopardy in Process Hazard Analysis

Allison De Man
&
Guillermo Pacanins

RISK CONSULTING | EDUCATION SERVICES | SAFEGUARD PROFILER | SAFEGUARD SENTINEL
## Introduction to Process Hazard Analysis

<table>
<thead>
<tr>
<th>Cause</th>
<th>Case Number</th>
<th>Consequence</th>
<th>Gas Limits</th>
<th>Safety</th>
<th>CAT</th>
<th>Gas Data</th>
<th>CAT</th>
<th>Recommendation</th>
<th>Responsible</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-H2S fatalities expected</td>
<td>PP-4-2020-01</td>
<td>1.1.1.1</td>
<td>Loss of human life and property</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PP-4-2020-02</td>
<td>1.1.1.2</td>
<td>Loss of human life and property</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PP-4-2020-03</td>
<td>1.1.1.3</td>
<td>Loss of human life and property</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PP-4-2020-04</td>
<td>1.1.1.4</td>
<td>Loss of human life and property</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Remarks:**
- 1: Fatality in low risk/low action required.
- 2: Control is not an option/low risk.
- 3: Control is not an option/low risk.
- 4: Control is not an option/low risk.
Initiating Event Types

External Events
- Earthquakes, tornadoes, hurricanes, or floods
- Airline crashes
- Major accidents in adjacent facilities
- Sabotage or terrorism

Equipment Failures
- Control Systems
  - Software bugs
  - Component failures
- Mechanical Systems
  - Wear
  - Corrosion
  - Vibration
  - Defects
  - Use outside design limits

Human Failure (Commission and Omission)
- Operational error
- Maintenance error
- Critical response error
- Programming error

FIGURE 5.1. Types of initiating events.
Purpose of a HAZOP Study

- HAZOP team must methodically identify, as much as possible, all the credible initiating events
- Ensure that the resulting hazardous scenarios have adequate safeguards or recommendations to reduce the risk to a tolerable level

But what is considered credible?
History of Double Jeopardy

- Legal term that appeared in the Fifth Amendment of the U.S. Constitution
  - Prevents a person from being tried in court twice for the same offense

- In the context of a PHA session:
  - Double jeopardy prevents the analysis of two or more independent failures that occur concurrently
    - Tank agitator fails – Equipment failure
    - Add too much catalyst – Human Failure

- Key factors to consider when calling a multiple failure scenario double jeopardy in a PHA
  - Independence
  - Revealed of Unrevealed
  - Resulting Consequence Severity
Independence of Initiating Events

- Independence is one of the most important factors to consider when deciding if a scenario is a double jeopardy scenario or not.

- If the multiple failures are found to be independent then the scenario may be deemed as a double jeopardy scenario.

- However, if the scenarios are found to be dependent, these scenarios would be credible to analyze in the HAZOP session.
Dependency Between Initiating Events

• Is there a potential failure elsewhere in the system that can lead to a multiple event failure?

• Common cause failures
  • Provides a link of dependency between two initiating event failures.
  • Loss of utilities: power, instrument air, water, etc...
  • Maintenance procedure errors - incorrect orientation of multiple valves after shutdown

Importance of considering loss of utilities and start-up/shutdown modes in the HAZOP study.

Multiple concurrent initiating event failures can be credible

Should be analyzed in the HAZOP study
Probability of Occurrence for Concurrent Independent Failures

Multiple the failure rate of each independent case to get an approximation of the probability of the multiple failures occurring concurrently.

<table>
<thead>
<tr>
<th>Probability of Failure of A = 10^-2/year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of Failure of B = 10^-2/year</td>
</tr>
</tbody>
</table>

When A and B are independent failures, an approximation of the probability of occurring concurrently is

\[ P(A \text{ and } B) = P(A) \times P(B) = 10^{-2} \times 10^{-2} = 10^{-4}/\text{year} \]

Rare Event Approximation
Revealed or Unrevealed Failure

• Is the failure revealed or detected shortly after the failure occurs?

• If the failure remains unrevealed for long enough that a second failure also occurs, then double jeopardy is not applicable
  • Multiple failure scenario needs to be considered in the PHA.

• Latent failures - do not have an immediate effect on the system when the failure occurs
  • Normally opened valve that fails in the open position.
  • Failure not detected until that valve is needed to close on demand.

• Exposure Time – includes detection time and time to correct the failure
  • Long durations of corrective action can lead to the credible occurrence of another independent initiating event
Probability of Occurrence of Credible Concurrent Failures

- When one initiating event is a **latent** failure, add the failure rate of each independent case to determine the probability of occurrence of the multiple failure case

<table>
<thead>
<tr>
<th>Event</th>
<th>Probability of Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>$10^{-2}$/year</td>
</tr>
<tr>
<td>B</td>
<td>$10^{-2}$/year</td>
</tr>
</tbody>
</table>

When **A** and **B** are independent failures, but one failure is unrevealed the probability of occurring concurrently is

$$P(\text{A and B}) = P(A) + P(B) = 10^{-2} + 10^{-2} = 2 \times 10^{-2}/\text{year}$$

This scenario is still very probable to occur and the concurrent failure should therefore be considered in the HAZOP
Consequence Severity of the Independent Concurrent Failure Scenario

• Probability of occurrence of two concurrent independent initiating events is typically very low (rare event approximation)

• However, the severity of the multiple failure hazardous event can very severe, even more severe than each independent event failure

• The resulting risk level may need to be analyzed in the HAZOP session
  • If not addressed in the HAZOP then these high risk scenarios will also miss being addressed Layer of Protection Analysis (LOPA) or Qualitative Risk Assessment (QRA).
Consequence Severity of the Independent Concurrent Failure Scenario

- Assume that the mitigations put in place to protect against one independent failure should also help to mitigate against the concurrent failure of two independent events.

- The resulting increased severity and risk level may mean these safeguards are now inadequate and the increased severity scenario is left with an unacceptable level of risk.

- Safeguards can also be deemed unnecessary (overprotection) for the lower severity independent failure case and not listed as mitigation.
  - Safeguards would then be missed when identifying critical safeguards.
What Examples are NOT Double Jeopardy

- Already addressed Common Cause Failures and Latent Failures

- Chain Reaction events
  - One failure triggering another failure
  - Failures occur sequentially one after another

- Failure of a Safeguard or IPL
  - Lack of response of a safeguard(s) is already taken into consideration when developing the hazardous event scenario
  - The hazardous scenario only occurs if the safeguard(s) fails

- Knock-on Effects
  - Events that occur as the result of failure events in other process units/areas
  - Include impacts from fire, explosion, loss of containment, etc.

- Failure of conditional enablers or modifiers
  - Conditional failures do not initiate a hazardous scenario by themselves
What Examples are Double Jeopardy

• Two separate independent and concurrent initiating events that lead to a cause of deviation from the intended design.
  • Independent
  • Revealed
  • Do not result in an extremely high consequence severity
Case Study – Bayer CropScience Explosion

• August 28, 2008, an explosion at a Bayer CropScience pesticide manufacturing facility in West Virginia killed two workers and injured eight

• The explosion was the result of a runaway chemical reaction inside a pressure treater vessel
Case Study – Bayer CropScience Explosion

• Independent initiating events (both human failures):
  • A high concentration of methomyl-containing solvent was sent to the treater
  • The failure to pre-fill the treater with clean solvent.

The concurrent occurrence of these two independent initiating events along with the failure or inadequacy of the safeguards present lead to the runaway reaction and resulting explosion.

• No PHA conducted
• Safeguards for the independent failure case were inadequate for the multiple failure scenario
• Would a HAZOP had identified these failures?
Process Safety Management Root Causes

Bayer CropScience Explosion Root Cause

*Significant pressure within the company to resume production even though the system maintenance was not completed*

- Double jeopardy is only applicable at the process level

- HAZOP only identifies the cause-consequence pair scenarios at the physical process level

- For major accidents half a dozen root and contributing causes were identified as playing a part in the occurrence of the major accident
Process Safety Management Root Causes

Societal
- Sustainable Risk
- Market Forces
- Values, Attitude

Governance/Regulatory System
- Corporate Regulatory System
- Govt. Codes of Federal Regulations, CFR
- Govt. CFR - OSHA
- Govt. CFR - EPA

Corporate Facilities
- Risk Assessment
- Process Safety Audit
- Cost Cutting
- Conduct
- Privacy
- Insurance

Organizational
- Presence of engineers
- Focus on LTs
- Engineering design
- Monitoring Process Safety

Operational Management
- Employee Participation
- Process Safety Information
- Process Hazards Analysis
- Operating Procedures
- Training
- Contractors
- Pre-Startup Safety Review

- Mechanical Integrity
- Hot Work Permit
- Management of Change
- Incident Investigation
- Emergency Planning
- Audits & Assessments
- Safe Work Practice

AcciMap (causal diagram)

Lessons from Longford The Esso Gas Plant Explosion, Andrew Hopkins
Process Safety Management Root Causes

- PSM root causes can add credibility to independent concurrent multiple failure cases.

- PHAs are not the place to discuss or identify the presence of PSM issues.

No matter how detailed or meticulous the PHA itself is, there still can be underlying organizational PSM issues that can affect the physical root cause of a major incident.
Conclusions

• Double jeopardy is an important part of PHA studies

• Knowing when double jeopardy can and cannot be considered is crucial to ensure that credible scenarios are not getting overlooked

• There are three questions that one should ask when deciding if a scenario should be considered double jeopardy or not
Conclusions – Three Questions to ask

1. Are the initiating events independent or is there a common cause failure that could lead to both failures occurring?

2. Are the failures revealed failures? Would you know if one of the failures occurred, or could one failure be a latent failure that remains undetected?

3. Is the resulting consequence severity of the concurrent independent failures high enough to be considered an extreme risk?

If the initiating event failures are independent, revealed and do not result in a high consequence severity, then the concurrent initiating event failures are considered to be double jeopardy and do not need to be analyzed further in the PHA.